# Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
a facial scan sensor configured to detect a proffered facial scan sample, said facial scan sensor configured to communicate with said system; and,
a device configured to verify said proffered facial scan sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said facial scan sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said facial scan sensor is configured to log at least one of a detected facial scan sample, processed facial scan sample and stored facial scan sample.

[c5] The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered facial scan samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, wherein said facial scan sensor device is configured with at least one of an optical scanner, imaging radar, ultraviolet imaging system and video camera.

[c9] The smartcard transaction system of claim 1, wherein said facial scan sensor device is configured to detect and verify facial scan characteristics including at least one of nodal points, the distance between the eyes, the width of the nose, the jaw line, forehead slope, lip shape, distance between the ears and the depth of the eye sockets.

[c10] The smartcard transaction system of claim 1, wherein said facial scan sensor device is configured to detect and verify pupil dilation, pressure, blinking, motion, and body heat.

[c11] The smartcard transaction system of claim 1, further including a device configured to compare a proffered facial scan sample with a stored facial scan sample.

[c12] The smartcard transaction system of claim 11, wherein said device configured to compare a facial scan sample is at least one of a third-party security vendor device and local CPU.

[c13] The smartcard transaction system of claim 11, wherein a stored facial scan sample comprises a registered facial scan sample.

[c14] The smartcard transaction system of claim 13, wherein said registered facial scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c15] The smartcard transaction system of claim 14, wherein different registered facial scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c16] The smartcard transaction system of claim 14, wherein a facial scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a facial scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said

second user information is different than said first user information.

[c17] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered facial scan sample.

[c18] The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered facial scan sample.

[c19] The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c20] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c21] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c22] A method for facilitating biometric security in a smartcard transaction system comprising: proffering a facial scan to a facial scan sensor communicating with said

system to initiate verification of a facial scan sample for facilitating authorization of a transaction.

[c23] The method for of claim 22, further comprising registering at least one facial scan sample with an authorized sample receiver.

[c24] The method of claim 23, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a facial scan to said authorized sample receiver, processing said facial scan to obtain a facial scan sample, associating said facial scan sample with user information, verifying said facial scan sample, and storing said facial scan sample upon verification.

[c25] The method of claim 22, wherein said step of proffering includes proffering a facial scan to at least one of an optical scanner and video camera.

[c26] The method of claim 22, wherein said step of proffering further includes proffering a facial scan to a facial scan sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said facial scan sample.

[c27] The method of claim 22, wherein said step of proffering a facial scan to a facial scan sensor communicating with

said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c28] The method of claim 22, wherein said step of proffering a facial scan to a facial scan sensor communicating with said system to initiate verification further includes comparing a proffered facial scan sample with a stored facial scan sample.

[c29] The method of claim 28, wherein said step of comparing includes comparing a proffered facial scan sample to a stored facial scan sample by using at least one of a third-party security vendor device and local CPU.

[c30] The method of claim 28, wherein said step of comparing includes comparing nodal points.

[c31] The method of claim 30, wherein said step of comparing nodal points comprises storing, processing and comparing at least one of the distance between the eyes, the width of the nose, the hairline, the jaw line, forehead slope, lip shape, distance between the ears and the depth of the eye sockets.

[c32] The method of claim 22, wherein said step of proffering

a facial scan to a facial scan sensor communicating with said system further comprises using said facial scan sensor to detect at least one of pupil dilation, pressure, motion, and body heat.

[c33] The method of claim 22, wherein said step of proffering a facial scan to a facial scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered facial scan sample

[c34] The method of claim 22, wherein said step of proffering a facial scan to a facial scan sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c35] A method for facilitating biometric security in a smartcard transaction system comprising:
detecting a proffered facial scan at a sensor communicating with said system to obtain a proffered facial scan sample;
verifying the proffered facial scan sample; and
authorizing a transaction to proceed upon verification of the proffered facial scan sample.

[c36] The method of claim 35, wherein said step of detecting further includes detecting a proffered facial scan at a

sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c37] The method of claim 35, wherein said step of detecting a proffered facial scan includes detecting a proffered facial scan at one of a video camera and optical scanner.

[c38] The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered facial scan sample.

[c39] The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered facial scan samples during a transaction.

[c40] The method of claim 35, wherein said step of detecting further includes logging each proffered facial scan sample.

[c41] The method of claim 35, wherein said step of detecting further includes at least one of detection, processing and storing at least one second proffered facial scan sample.

[c42] The method of claim 35, wherein said step of detecting further includes using said facial scan sensor to detect at least one of pupil dilation, pressure, motion, and body heat.

[c43] The method of claim 35, wherein said step of verifying

includes comparing a proffered facial scan sample with a stored facial scan sample.

[c44] The method of claim 43, wherein said step of comparing a proffered facial scan sample with a stored facial scan sample comprises storing, processing and comparing at least one nodal point.

[c45] The method of claim 43, wherein comparing a proffered facial scan sample with a stored facial scan sample includes comparing a proffered facial scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c46] The method of claim 35, wherein said step of verifying includes verifying a proffered facial scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c47] The method of claim 35, wherein said step of verifying includes verifying a proffered facial scan sample using one of a local CPU and a third-party security vendor.